



# HONEYWELL FORGE CYBERSECURITY+ | CYBER WATCH

## PRODUCT INFORMATION NOTE

Honeywell Forge Cybersecurity+ | Cyber Watch, designed to address the multi-site capabilities and governance requirements that Chief Information Security Officers (CISOs) seek in a cybersecurity solution.

This innovative offering transcends the ordinary by placing a focus on the specific demands of CISOs overseeing multi-site operations and governance. Honeywell Forge Cybersecurity+ | Cyber Watch is designed to empower these leaders with a wealth of actionable information for OT cybersecurity. Offering unparalleled multi-site capabilities and governance features, this vendor-neutral solution is designed to provide CISOs access to both real-time and historical data, encompassing identified assets, threats, and vulnerabilities. By harnessing these robust capabilities, this solution tailored to help CISOs effectively reduce cyber risks, to provide seamless continuity of operations across their expansive industrial landscape, and to keep up with the ongoing change in cybersecurity regulations.



## KEEP WATCH OVER YOUR CYBERSECURITY POSTURE ACROSS ALL SITES

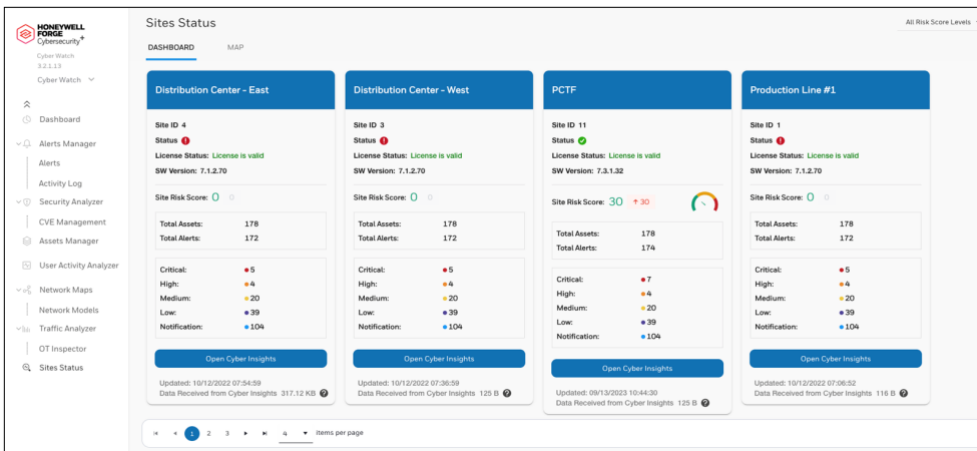
Cyber Watch is a software-led solution designed to help users get an enterprise (multi-site) view of their OT cybersecurity posture and better manage their cyber risks and compliance across all operating sites. Cyber Watch is designed to aggregate data from Cyber Insights installations at each site, thereby helping a user keep watch of their cybersecurity posture across all sites. It is designed to provide a centralized view into OT cyber threats and to help users more quickly identify, prioritize, and respond to signs of

compromise. Cyber Watch includes an optional Governance Dashboard that is capable of enabling a user to know both organizational and industry related cybersecurity compliance status at any point in time. Cyber Watch is also capable of being connected to many other enterprise corporate solutions such as a SIEM and a SOC incident management dashboard.

## MULTI-SITE CAPABILITIES

Cyber Watch is highly scalable and can support hundreds of locations managed centrally via the multi-site solution. It is designed so that data from all sites is centrally aggregated, including full asset inventory, traffic, and alerts data.

### *Cyber Watch Multi-site Dashboard*



Workflows such as alert handling and central site configuration are also available. The Cyber Watch solution is designed so that all software updates provided as part of technical support are automatically pushed to the managed locations.

## GOVERNANCE AND COMPLIANCE

Cyber Watch also offers an optional product that addresses a user's need for compliance with organizational policies and industry regulations: The Cyber Watch Governance Dashboard.

The Cyber Watch Governance Dashboard is engineered to enable a user's IT and audit departments to centrally define and monitor the organization's adherence to company policies and OT- related standards and regulations such as IEC 62443, the NIST framework, and most major compliance framework for OT. This functionality can enable CISOs to plan their cybersecurity strategy and report and measure their organization's compliance based on the actual data derived from the networks.

Configured and managed centrally, the Cyber Watch Governance Dashboard is designed to provide a user the ability to define a holistic organizational policy— compliance to regulations and to organizational policies. It then capable of tracking and measuring compliance and monitoring the progress made over time across distributed sites. It also includes the ability to support incremental, time-based changes.

The compliance status is displayed on detailed dashboards and reports. The Cyber Watch Governance Dashboard is designed to determine compliance status based on actual network traffic, instead of relying on historical data or on estimations. It is also designed to provide users an alert when an attack happens globally.

The Governance Dashboard also includes the capability to receive weekly updates on security trends in the world where the updates are in the form of reputation (malicious IP, DNS, and file hashes) and as a report. The report is relevant to the specific site according to 6 parameters: (1) Industry, (2) Country, (3) Vendor, (4) Device Type, (5) CVE, and (6) Protocols.

## FEATURES AND BENEFITS



### DESIGNED TO PROVIDE THE FOLLOWING:

**Central Security Management** – Get access to know cyber threats at an individual site or across multiple sites and centralize the coordination of response. Cyber Watch is highly scalable and can support up to hundreds of distributed sites managed centrally via the multi-site portal.

**Central Governance** - Continuously monitor your remote sites' adherence to industry standards IEC 62443, NERC CIP, NIST, ISO 27001 and others, and organizational policies.

**Automate Site Management** – Central configuration management, central licensing, automated software updates, and more.



### DESIGNED TO PROVIDE THE FOLLOWING:

**Always Up To Date** - Based on real time data extracted from your network. Provides continuous, real-time visibility to the adherence of regulations and industry frameworks.

**Improves Over Time** - Track improvement of organizational compliance over time.

**Reporting** - Automatically generate compliance reports for executive and on-site teams.

**MSP Ready** – Public or private cloud enabled. Manage multiple organizations / customers with secure, full data segregation and more).



### DESIGNED TO PROVIDE THE FOLLOWING:

**Reporting** - Automatically generate compliance reports for executive and on-site teams.

**Reduce Costs** - Centrally managing the governance of an organization's remote sites, eliminates the need for travel and on-site audits.

**MITRE ATT&CK Framework** - The Cyber Watch MITRE ATT&CK framework enables security professionals to move beyond identifying the most common attack methods.

## WHY HONEYWELL?

Honeywell has more than 100 years of experience in the industrial sector and more than 20 years of experience in industrial cybersecurity and thousands of projects delivered world-wide. We provide cybersecurity solutions that protect industrial assets' availability, safety and reliability worldwide. Honeywell's complete portfolio includes cybersecurity software, managed security services, industrial security consulting and integrated security solutions. We combine industry-leading cybersecurity experience with decades of process control knowledge to provide the premier industry solutions for an operational technology environment.

*This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. Any descriptions of future product direction, intended updates, or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion.*

*All pictures shown in this document are for illustration purposes only; the actual product may vary.*

*Honeywell® is a trademark of Honeywell International Inc. Other brand or product names are trademarks of their respective owners.*

### **For More Information**

To learn more about Cyber Watch visit [HoneywellForge.ai](https://www.honeywell.com/cyberwatch) or contact your Honeywell account manager.

### **Honeywell Connected Enterprise**

715 Peachtree Street NE  
Atlanta, Georgia 30308